UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/633,918	08/04/2003	Hamdy Soliman	NMTECH13.CIP2	4945

30996 7590 10/02/2006

ROBERT W. BECKER & ASSOCIATES
707 HIGHWAY 333
SUITE B
TIJERAS, NM 87059-7507

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/633,918	SOLIMAN, HAMDY	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Nonstatutory Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-20 of application 10/633918 is provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17, 35-36 of copending Application No. 10/387711. Although the conflicting claims are not identical, they are not patentably distinct from each other see below for rationale.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Application 10/633918 Claim 1	Application 10/387711 Claim 1
A method of providing a secure data stream between system nodes the method comprising	A method of providing a secure data stream between system nodes the method comprising
Encrypting data at a node with an encryption key,	Creating data at a node
Regenerated a new encryption key at a node with an encryption key and selected encrypted data	Regenerated a new encryption key at a node using created data and a previous encryption key

3. Claim 1(10/633918) which claims encrypting data at a node with an encryption key, is obvious over Claim 1(10/387711) which claims creating data at a node, because in order to encrypted data, it must first be created.

4. Claim 1(10/633918) which claims regenerated a new encryption key at a node with an encryption key and selected encrypted data, is obvious over Claim 1(10/387711) which claims regenerated a new encryption key at a node using created data and a previous encryption key and selected data, because, the created data must be created in order to use the selected data as part of the new encryption key.

5. Further, Claim 19(10/633918) recites same limitations as Claim 35(10/387711), except for the last limitation "using selected previously encrypted data"(10/633918), with "using data from the data stream"(10/387711). It is obvious that the selected previously encrypted data, is

the same as using data from the data stream, because the data from the data stream is the old data before regeneration method, thus this is the previously encrypted data.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Guski et al(6,292,896).

8. As per claim 1, Guski et al. discloses a method of providing a secure data stream between system nodes(ref# 102, 104, fig. 1, sheet 1, col. 3, lines 48-57, fig. 3 sheet 2 and associated descriptions, col. 4, lines 26-32), encrypting data at a node with an encryption key(see col. 4, lines 26-32, 65-67); selecting encrypted data; and regenerating a new encryption key at a node with an encryption key and selected encrypted data(see col. 9, lines 11-34, 44-50).

9. As per claim 2, Guski discloses wherein the step of selecting encrypted data includes selecting encrypted data using a byte from a previous encryption key as a seed of random generation (see col. 9, lines 25-67, col. 10, lines 1-13).

10. As per claim 3, Guski discloses wherein the step of regenerating a new encryption key includes regenerating a new encryption key by performing a logic operation on a previous encryption key and selected encrypted data(see col. 9, lines 25-34, 44-50).

11. As per claim 4, Guski discloses wherein the step of regenerating a new encryption key by

performing a logic operation includes regenerating a new encryption key by performing an XOR logic operation on a previous encryption key and selected encrypted data(col. 9, lines 44-50).

12. As per claim 5, Guski discloses wherein the step of regenerating a new encryption key by performing a logic operation includes performing a logic operation on a previous encryption key and selected encrypted data to form an expanded key(see col. 9, lines 25-34, 52-58).

13. As per claim 6, Guski discloses the step of selecting bytes from an expanded key to generate the new encryption key(see col. 9, lines 25-58).

14. As per claim 7, Guski discloses wherein the step of selecting bytes from an expanded key to generate the new encryption key includes randomly selecting bytes from an expanded key to generate the new encryption key(see col. 9, lines 25-34).

15. As per claim 8, Guski discloses wherein the step of randomly selecting bytes from an expanded key to generate the new encryption key comprises randomly selecting bytes from an expanded key using a byte from a previous encryption key as a seed of random generation (see col. 9, lines 25-34, 59-65).

16. As per claim 9, Guski discloses the step of encrypting data with a new encryption key(see col. 9, lines 25-34).

17. As per claim 10, Guski discloses wherein the step of encrypting data with a new encryption key includes performing a logic operation on the data and new encryption key(see col. 9, lines 25-34, 44-51).

18. As per claim 11, Guski discloses wherein the step of performing a logic operation on the data and new encryption key includes performing an XOR operation on the data and new encryption key(see fig. 8 sheet 6, col. 9, lines 44-51).

19. As per claim 12, Guski discloses wherein the step of performing a logic operation on the data and new encryption key includes forming a cipher(col. 9, lines 44-51).

20. As per claim 13, Guski discloses the step of permuting portions of the cipher to form another cipher(see col. 9, lines 44-51).

21. As per claim 14, Guski discloses the step of transmitting encrypted data over a data stream(see fig. 3 sheet 2, col. 4, lines 26-32).

22. As per claim 15, Guski discloses the step of receiving encrypted data at a destination node(see fig. 3 sheet 2, col. 4, lines 26-32).

23. As per claim 16, Guski discloses the step of decrypting encrypted data at the destination node(see col. 4, lines 65-67).

24. As per claim 17, Guski discloses wherein the step of decrypting encrypted data includes decrypting with a decryption key(see col. 4, lines 26-32, 65-67).

25. As per claim 18, Guski discloses the step of regenerating a new decryption key using selected decrypted data and a previous decryption key, because Guski encryption/decryption key(session keys) are a key pair, and both nodes in Guski are synchronized with the same key(see col. 12, lines 17-27). Thus, when a new encryption key is regenerated the decryption key will be regenerated also(see col. 9, lines 25-34) .

26. As per claim 19, Guski discloses a system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus(see fig. 3, sheet 2),: a source programmable apparatus; a data stream created by said source programmable apparatus; means for encrypting data of said data stream with an encryption key(see col. 4, lines 26-32, 65-67); and means for regenerating a new encryption key using selected previously encrypted

data(see col. 9, lines 11-34, 44-50).

27. As per claim 20, Guski discloses a destination programmable apparatus in electrical communication with said source programmable apparatus(see fig. 3 sheet 2); means for transmitting encrypted data to said destination programmable apparatus(see fig. 3 sheet 2); means for decrypting said encrypted data received at said destination programmable apparatus with a decryption key; and means for regenerating a new decryption key using selected previously decrypted data(see col. 4, lines 26-32, 65-67, col. 9, lines 25-34, col. 12, lines 17-27).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 24, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/27/06